AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently amended) A computer implemented method of detecting scanning attacks, comprises:

adding host-pair connection records to a first data structure stored on a computer readable medium when a host accesses another host during a first update period;

determining the number of new host pairs added to the first data structure over the first update period;

aggregating host-pair connection records from the first data structure into a second data structure which corresponds to a second update period that is greater than the first update ~~period;~~period, wherein aggregating host-pair connection records involves partitioning hosts into groups that have similar connection habits;

determining the number of new host pairs added to the second data structure over the second update period; and

indicating a host as a scanner when at least one of the following conditions is true:

(1) the host appears in more than a first threshold number of host pairs within the first update period, and a first historical number of host pairs is smaller than the first threshold number by a first factor value; and

(2) the host appears in more than a second threshold number of host pairs within the second update period, and a second historical number of host pairs is smaller than the second threshold number by a second factor value.

2. (Previously presented) The method of claim 1 wherein the first threshold number and the first factor value are adjustable.

3. (Previously presented) The method of claim 2 wherein the first data structure is a current time-slice connection table and host-pair connection records are added to the current time slice connection table.

4. (Previously presented) The method of claim 3, further comprising:

checking for ping scans at the end of the second update period; and

indicating hosts which produced more than the second threshold number of new host pairs over the second update period.

5. (Cancelled)

6. (Previously presented) The method of claim 1 further comprising:

maintaining Address Resolution Protocol (ARP) packet statistics in the first data structure and for sparse subnets tracking the number of generated ARP requests that do not receive responses to detect scans on sparse sub-networks.

7. (Original) The method of claim 1 wherein the scanning attack is a ping scanning attack.

8. (Currently amended) A computer implemented method of detecting port scanning attacks, the method comprises:

retrieving from a first data structure stored on a computer readable medium logged values of protocols and ports in host-pair connection records added in the first data structure during a first update period;

determining the number of ports associated with a host over the first update period based on the host-pair connection records in the first data structure;

aggregating host-pair connection records from the first data structure into a second data structure which corresponds to a second update period that is greater than the first update ~~period;~~ period, wherein aggregating host-pair connection records involves partitioning hosts into groups that have similar connection habits;

determining the number of ports associated with a host over the second update period based on the host-pair connection records in the second data structure; and

reporting a host associated with a port scan when at least one of the following conditions is true:

(1) the number of ports associated with the host within the first update period is greater than a first threshold number, and a first historical number of ports associated with the host is smaller than the first threshold number by a first factor value; and

(2) the number of ports associated with the host within the second update period is greater than a second threshold number, and a second historical number of ports associated with the host is smaller than the second threshold number by a second factor value.

9. (Original) The method of claim 8 further comprising:

assigning a severity level to the port scan and reporting the severity level of the port scan.

10. (Original) The method of claim 8 wherein the reported severity varies as a function of the deviation from historical norm.

11. (Previously presented) The method of claim 8 further comprising:

determining from accessing data in the first data structure, statistics about TCP reset (RST) packets and ICMP port-unreachable packets, to detect a spike in the number of RST packets and ICMP port-unreachable packets to determine the severity of a port scan event.

12. (Cancelled)

13. (Cancelled)

14. (Currently amended) A computer program product residing on a computer readable medium for detecting scanning attacks, comprises instructions for causing a computer to:

add host-pair connection records to a first data structure when a host accesses another host during a first update period;

determine the number of new host pairs added to the first data structure over the first update period;

aggregate host-pair connection records from the first data structure into a second data structure which corresponds to a second update period that is greater than the first update ~~period;~~ period, wherein aggregating host-pair connection records involves partitioning hosts into groups that have similar connection habits;

determine the number of new host pairs added to the second data structure over the second update period; and

indicate a host as a scanner when at least one of the following conditions is true:

(1) the host appears in more than a first threshold number of host pairs within the first update period, and a first historical number of host pairs is smaller than the first threshold number by a first factor value; and

(2) the host appears in more than a second threshold number of host pairs

within the second update period, and a second historical number of host pairs is smaller than the second threshold number by a second factor value..

15. (Previously presented) The computer program product of claim 14 wherein the first threshold number and the first factor value are adjustable .

16. (Previously presented) The computer program product of claim 14 wherein the first data structure is a current time-slice connection table and host-pair connection records are added to the current time slice connection table.

17. (Previously presented) The computer program product of claim 16, further comprising instructions to:

check for ping scans at the end of a the second update period; and

indicate hosts which produced more than the second threshold number of new host pairs over the second update period.

18. (Cancelled)

19. (Previously presented) The computer program product of claim 14 further comprising instructions to:

maintain Address Resolution Protocol (ARP) packet statistics in the first data structure; and

track the number of generated ARP requests that do not receive responses to detect scans on sparse sub-networks.

20. (Currently amended) A computer program product residing on a computer readable medium for detecting port scanning attacks, the computer program product comprises instructions for causing a processor to:

retrieve from a first data structure logged values of protocols and ports in host-pair connection records in the first data structure during a first update period;

determine the number of ports associated with a host over the first update period based on the host-pair connection records in the first data structure;

aggregate host-pair connection records from the first data structure into a second data structure which corresponds to a second update period that is greater than the first update ~~period;~~ period, wherein aggregating host-pair connection records involves partitioning hosts into groups that have similar connection habits;

determine the number of ports associated with a host over the second update period based on the host-pair connection records in the second data structure; and

report a host associated with a port scan when at least one of the following conditions is true:

(1) the number of ports associated with the host within the first update period is greater than a first threshold number, and a first historical number of ports associated with the host is smaller than the first threshold number by a first factor value; and

(2) the number of ports associated with the host within the second update period is greater than a second threshold number, and a second historical number of ports associated with the host is smaller than the second threshold number by a second factor value.

21. (Original) The computer program product of claim 20 further comprising instructions to:

assign a severity level to the port scan and report the severity level of the port scan.

22. (Original) The computer program product of claim 21 wherein the reported severity varies as a function of the deviation from historical norm.

23. (Previously presented) The computer program product of claim 21 further comprising instructions to:

determine from the first data structure statistics about TCP reset (RST) packets and ICMP port-unreachable packets to detect a spike in the number of RST packets and ICMP port-unreachable packets to determine the severity of a port scan event.

24. (Currently amended) Apparatus comprising:

circuitry for detecting scanning attacks, comprising:

circuitry to add host-pair connection records to a first data structure when a host accesses another host during a first update period;

circuitry to determine the number of new host pairs added to the first data structure over a first update period;

circuitry to aggregate host-pair connection records from the first data structure into a second data structure which corresponds to a second update period that is greater than the first update ~~period,~~ period, wherein aggregating host-pair connection records involves partitioning hosts into groups that have similar connection habits;

circuitry to determine the number of new host pairs added to the second data structure over the second update period; and

circuitry to indicate a host as a scanner when at least one of the following conditions is true:

(1) the host appears in more than a first threshold number of host pairs within the first update period, and a first historical number of host pairs is smaller than the first threshold number by a first factor value; and

(2) the host appears in more than a second threshold number of host pairs

within the second update period, and a second historical number of host pairs is smaller than the second threshold number by a second factor value.

25. (Previously presented) The apparatus of claim 24 wherein the first threshold number and the first factor value are adjustable.

26. (Previously presented) The apparatus of claim 24 wherein the first data structure is a current time-slice connection table and host-pair connection records are added to the current time slice connection table.

27. (Previously presented) The apparatus of claim 24, further comprising:

circuitry to check for ping scans at the end of a second update period; and

circuitry to indicate hosts which produced more than the second threshold number of new host pairs over the second update period.

28. (Currently amended) Apparatus comprising:

a processing device; and

a computer readable medium tangible embodying a computer program product for detecting scanning attacks, the computer program product comprising instructions for causing the processing device to:

add host-pair connection records to a first data structure when a host accesses another host during a first update period;

determine the number of new host pairs added to the first data structure over the first update period;

aggregate host-pair connection records from the first data structure into a second data structure which corresponds to a second update period that is greater than the first update ~~period;~~ period, wherein aggregating host-pair connection records involves partitioning hosts into groups that have similar connection habits;

determine the number of new host pairs added to the second data structure over the second update period; and

indicate a host as a scanner when at least one of the following conditions is true:

(1) the host appears in more than a first threshold number of host pairs within the first update period, and a first historical number of host pairs is smaller than the first threshold number by a first factor value; and

(2) the host appears in more than a second threshold number of host pairs within the second update period, and a second historical number of host pairs is smaller than the second threshold number by a second factor value..

29. (Previously presented) The apparatus of claim 28 wherein the first threshold number and the first factor value are adjustable.

30. (Previously presented) The apparatus of claim 28 wherein the first data structure is a current time-slice connection table and host-pair connection records are added to the current time slice connection table.

31. (Previously presented) The apparatus of claim 28, wherein the computer program product further comprises instructions to:

check for ping scans at the end of a second update period; and

indicate hosts which produced more than second threshold number of new host pairs over the second update period.

32. (Cancelled)

33. (Currently amended) Apparatus comprising:

a processing device;

a computer readable medium tangibly embodying a computer program product for detecting port scanning attacks, the computer program product comprises instructions for causing a processor to:

retrieve from a first data structure logged values of protocols and ports in host-pair connection records in the first data structure during a first update period;

determine the number of ports associated with a host over the first update period based on the host-pair connection records in the first data structure;

aggregate host-pair connection records from the first data structure into a second data structure which corresponds to a second update period that is greater than the first update ~~period;~~ period, wherein aggregating host-pair connection records involves partitioning hosts into groups that have similar connection habits;

determine the number of ports associated with a host over the second update period based on the host-pair connection records in the second data structure; and

report a host associated with a port scan when at least one of the following conditions is true:

(1) the number of ports associated with the host within the first update period is greater than a first threshold number, and a first historical number of ports associated with the host is smaller than the first threshold number by a first factor value; and

(2) the number of ports associated with the host within the second update period is greater than a second threshold number, and a second historical number of ports associated with the host is smaller than the second threshold number by a second factor value.

34. (Original) The apparatus of claim 33 further comprising instructions to:

assign a severity level to the port scan and report the severity level of the port scan.

35. (Previously presented) The apparatus of claim 34 wherein the reported severity varies as a function of the deviation from a historical norm.

36. (Previously presented) The apparatus of claim 34 further comprising instructions to:

determine from the first data structure statistics about TCP reset (RST) packets and ICMP port-unreachable packets to detect a spike in the number of RST packets and ICMP port-unreachable packets to determine the severity of a port scan event.

37. (Currently amended) A computer implemented method of detecting scanning attacks, comprises:

adding host-pair connection records to a first data structure stored on a computer readable medium when a host accesses another host during a first update period;

determining the number of new host pairs added to the first data structure over the first update period;

aggregating host-pair connection records from the first data structure into a second data structure which corresponds to a second update period that is greater than the first update ~~period;~~ period, wherein aggregating host-pair connection records involves partitioning hosts into groups that have similar connection habits;

determining the number of new host pairs added to the second data structure over the second update period; and

indicating a host as a scanner when the host appears in more than a first threshold number of host pairs within the first update period, and a first historical

number of host pairs is smaller than the first threshold number by a first factor value.

38. (Currently amended) A computer implemented method of detecting scanning attacks, comprises:

adding host-pair connection records to a first data structure stored on a computer readable medium when a host accesses another host during a first update period;

determining the number of new host pairs added to the first data structure over the first update period;

aggregating host-pair connection records from the first data structure into a second data structure which corresponds to a second update period that is greater than the first update ~~period;~~ period, wherein aggregating host-pair connection records involves partitioning hosts into groups that have similar connection habits;

determining the number of new host pairs added to the second data structure over the second update period; and

indicating a host as a scanner when the host appears in more than a second threshold number of host pairs within the second update period, and a second historical number of host pairs is smaller than the second threshold number by a second factor value.

39. (Currently amended) A computer implemented method of detecting port scanning attacks, the method comprises:

retrieving from a first data structure stored on a computer readable medium logged values of protocols and ports in host-pair connection records added in the first data structure during a first update period;

determining the number of ports associated with a host over the first update period based on the host-pair connection records in the first data structure;

aggregating host-pair connection records from the first data structure into a second data structure which corresponds to a second update period that is greater than the first update ~~period;~~ period, wherein aggregating host-pair connection records involves partitioning hosts into groups that have similar connection habits;

determining the number of ports associated with a host over the second update period based on the host-pair connection records in the second data structure; and

reporting a host associated with a port scan when the number of ports associated with the host within the first update period is greater than a first threshold number, and a first historical number of ports associated with the host is smaller than the first threshold number by a first factor value.

40. (Currently amended) A computer implemented method of detecting port scanning attacks, the method comprises:

retrieving from a first data structure stored on a computer readable medium logged values of protocols and ports in host-pair connection records added in the first data structure during a first update period;

determining the number of ports associated with a host over the first update period based on the host-pair connection records in the first data structure;

aggregating host-pair connection records from the first data structure into a second data structure which corresponds to a second update period that is greater than the first update ~~period;~~ period, wherein aggregating host-pair connection records involves partitioning hosts into groups that have similar connection habits;

determining the number of ports associated with a host over the second update period based on the host-pair connection records in the second data structure; and

reporting a host associated with a port scan when the number of ports

associated with the host within the second update period is greater than a second threshold number, and a second historical number of ports associated with the host is smaller than the second threshold number by a second factor value.